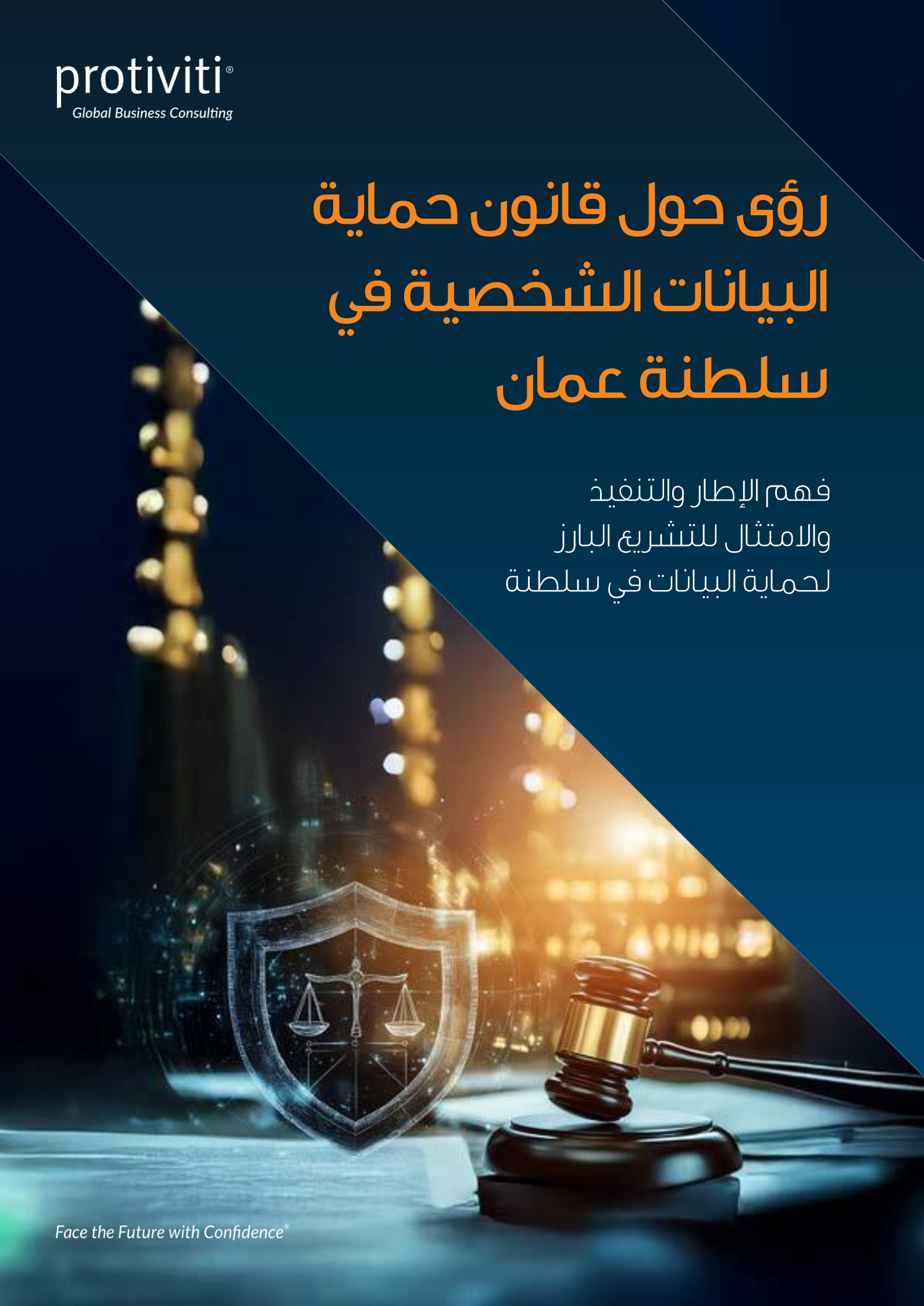
protiviti®
Global Business Consulting

رؤى حول قانون حماية البيانات الشخصية في سلطنة عمان

فهم الإطار والتنفيذ
والامتثال للتشريع البارز
لحماية البيانات في سلطنة



Face the Future with Confidence®

جدول المحتويات

المقدمة

يمثل قانون حماية البيانات الشخصية في سلطنة عمان خطوة رائدة في الحفاظ على حقوق الأفراد وتطبيق مبدأ المساءلة عند استخدام البيانات الشخصية في السلطنة. في وقت تتجه فيه المؤسسات بشكل متزايد نحو تحقيق التحول الرقمي والبنى التحتية الذكية وفق رؤية عمان 2040، يوفر قانون حماية البيانات الشخصية إطارًا شاملاً يعزز الثقة، ويقوي المساءلة، ويواكب الاتجاهات العالمية في مجال الخصوصية وحماية البيانات.

الامتثال لقانون حماية البيانات الشخصية في عمان ضروري من أجل:

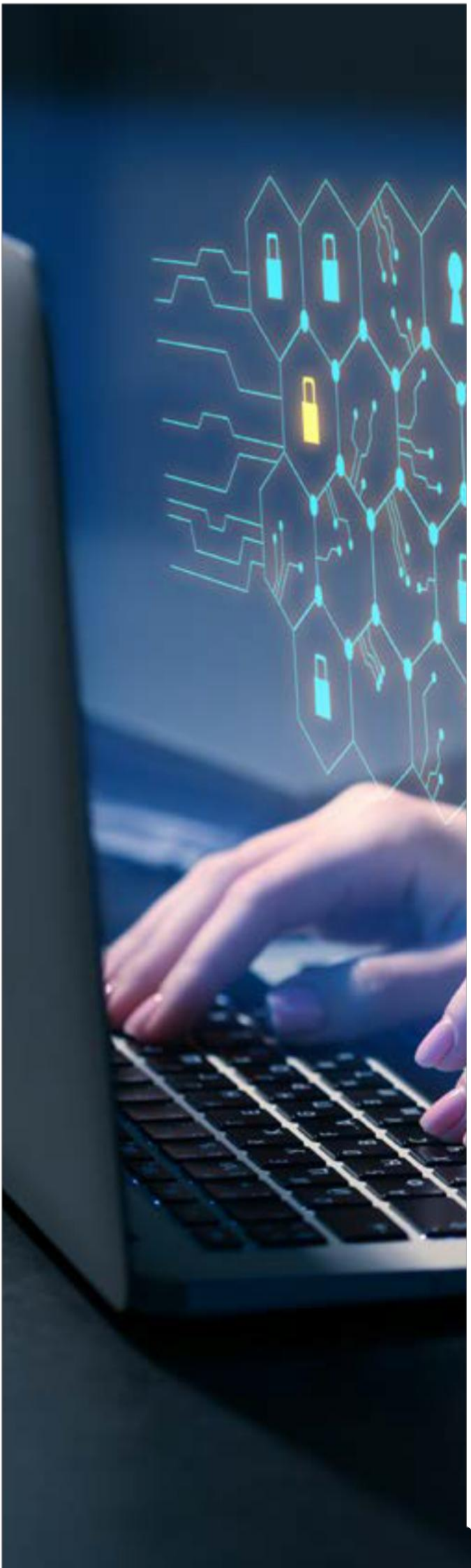
- بناء ثقة العملاء
- تعزيز قيمة العلامة التجارية للمؤسسة
- تحسين الميزة التنافسية
- التعامل الأمثل مع خروقات البيانات
- دعم الابتكار

في هذا المستند، نوضح نهجًا منظماً وفهمًا شاملاً للامتثال لقانون حماية البيانات الشخصية في سلطنة عمان. تعتمد منهجيتنا على دمج مجموعة واسعة من الخبرات القانونية والتنظيمية مع الخبرات العملية في التنفيذ، لضمان أن يصبح الامتثال لقوانين خصوصية البيانات جزءاً من جوهر المؤسسة وثقافتها.

نظرة عامة على القانون وخارطة التنفيذ

أصدرت سلطنة عمان قانون حماية البيانات الشخصية (ويُشار إليه فيما بعد باسم "قانون حماية البيانات الشخصية") بموجب المرسوم السلطاني رقم 2022/6، والمنشور في الجريدة الرسمية بتاريخ 13 فبراير 2022. وقد حل هذا القانون الشامل محل الأحكام السابقة المتعلقة بحماية البيانات الواردة في قانون المعاملات الإلكترونية، ودخل حيز التنفيذ رسميًا في 13 فبراير 2023. تتولى وزارة النقل والاتصالات وتقنية المعلومات (MTCIT) مسؤولية الإشراف والتنفيذ، مما يعكس التزام الحكومة بحماية البيانات الشخصية في ظل المشهد الرقمي المتطور بسرعة. لدعم تنفيذ القانون، صدرت اللائحة التنفيذية بموجب القرار الوزاري رقم 2024/34، اعتبارًا من 5 فبراير 2024. وفي يناير 2024، مددت الوزارة الموعد النهائي للامتثال حتى 5 فبراير 2026 بموجب القرار الوزاري رقم 2025/6، مما يمنح المؤسسات وقتًا إضافيًا للتوافق مع متطلبات القانون مع الحفاظ على الوضوح التنظيمي.

تستند المقالة التالية إلى قانون حماية البيانات الشخصية الصادر في فبراير 2022، وتدمج اللائحة التنفيذية التي تم إصدارها في فبراير 2024.



نطاق قانون حماية البيانات الشخصية

- ينطبق القانون على أي معالجة للبيانات الشخصية.
- تعني البيانات الشخصية أي معلومات تحدد شخصًا طبيعيًا بشكل مباشر أو غير مباشر، من خلال:
  - المعرفات مثل الاسم، الرقم المدني، الهويات الإلكترونية، أو بيانات الموقع الجغرافي؛
  - السمات المرتبطة بالهوية الجينية أو البدنية أو العقلية أو النفسية أو الاجتماعية أو الثقافية أو الاقتصادية.
- لا يقيّد القانون نطاقه بحسب القطاع أو طريقة المعالجة أو مصدر البيانات. وهذا يعني:
  - جميع أنواع البيانات الشخصية، بما في ذلك معلومات الاتصال والبيانات الصحية والمالية، مشمولة.
  - جميع مصادر البيانات الشخصية، سواء تم تقديمها مباشرة من الأفراد أو تم الحصول عليها من مصادر أخرى، مشمولة.
  - جميع أشكال البيانات الشخصية، سواء كانت إلكترونية أو ورقية أو منظمة أو غير منظمة، مشمولة.

ملاحظة: هذا الوصف للنطاق هو تفسير لقانون حماية البيانات الشخصية، حيث ينص القانون نفسه فقط على أنه ينطبق على معالجة البيانات الشخصية.

الإستثناءات بموجب القانون

يوفر قانون حماية البيانات الشخصية حالات محددة لا تنطبق فيها متطلباته. تهدف هذه الاستثناءات إلى تحقيق التوازن بين حقوق الخصوصية الفردية والمصالح الوطنية والقانونية والمجتمعية الأوسع. لا ينطبق قانون حماية البيانات الشخصية في الحالات التالية:

1. لحماية الأمن الوطني أو المصلحة العامة.
2. المعالجة من قبل الهيئات الحكومية أو الكيانات العامة كجزء من واجباتها القانونية.
3. للامتثال لالتزام قانوني أو حكم قضائي أو قرار رسمي.
4. لحماية المصالح الاقتصادية أو المالية للدولة
5. .لحماية مصلحة حيوية لصاحب البيانات.
6. للكشف عن الجرائم أو منعها، بناءً على طلب رسمي من سلطات التحقيق.
7. لتنفيذ عقد مع صاحب البيانات
8. المعالجة التي تتم في نطاق شخصي أو عائلي.
9. لأغراض البحث أو الإحصاء (التاريخية أو العلمية أو الأدبية أو الاقتصادية)، بشرط عدم إمكانية تحديد الأفراد في النتائج المنشورة.
10. بالنسبة للبيانات المتاحة للعامة، حيث لا يتعارض استخدامها مع قانون حماية البيانات الشخصية.

الغرامات بموجب القانون

تم وضع قانون حماية البيانات الشخصية بهدف ضمان المساءلة والامتثال. وتتمتع وزارة النقل والاتصالات وتقنية المعلومات بسلطة فرض العقوبات الإدارية على المؤسسات التي تنتهك أحكام قانون حماية البيانات الشخصية أو لوائحه التنفيذية. وتشمل هذه العقوبات ما يلي:

1. تحذير رسمي – يُصدر كإشعار رسمي لمعالجة عدم الامتثال.
2. تعليق التفويض – مؤقت حتى يتم تصحيح المخالفة.
3. الغرامات الإدارية – عقوبات مالية تصل إلى 2,000 ريال عماني (ألفي ريال عماني) عن كل مخالفة.
4. إلغاء التفويض – دائم في حالات عدم الامتثال الجسيم أو المتكرر

العقوبات بموجب القانون

قد تؤدي انتهاكات القانون إلى فرض عقوبات تتراوح بين 500 ريال عماني و500,000 ريال عماني، وذلك حسب النص المحدد الذي تم خرقه، مع تطبيق عقوبات أعلى على الانتهاكات الجسيمة مثل التحويلات غير المشروعة عبر الحدود أو المخالفات التي تشمل الأشخاص الاعتباريين.

العناصر الأساسية للقانون

المتطلبات الأساسية لقانون حماية البيانات الشخصية تشمل مجالات متعددة، بما في ذلك إدارة المخاطر، الامتثال، الالتزامات القانونية، حماية البيانات، حوكمة البيانات، وإدارة السجلات، بما يضمن التعامل المسؤول والشفاف مع البيانات الشخصية.

ومن المهم أن القانون يعكس أفضل الممارسات العالمية في مجال حماية البيانات، مما يضع سلطنة عمان في توافق مع المعايير الدولية للخصوصية والثقة، مع مراعاة السياق الوطني. بالنسبة للمنظمات، يتطلب ذلك اعتماد نهج شامل ومنظم وتعاوني لإنشاء برامج خصوصية قوية تعزز الثقة الرقمية، وتدعم الابتكار، وتزيد من القدرة التنافسية في اقتصاد يعتمد بشكل متزايد على البيانات.

الالتزامات الأساسية بموجب القانون

التزامات الخصوصية

- الالتزام بمبادئ الخصوصية الأساسية، بما في ذلك على سبيل المثال لا الحصر تقليل البيانات، تحديد مدة التخزين، جودة البيانات، والأمان.
- الحصول على موافقة صريحة كأساس قانوني رئيسي لمعالجة البيانات الشخصية.
- ضمان قدر أكبر من الشفافية للأفراد بشأن كيفية جمع بياناتهم واستخدامها ومشاركتها.
- تعزيز حقوق الأفراد، بما في ذلك الحق في الإعلام، الوصول، التصحيح، والإشعار بوقوع خرق.

التزامات إدارة السجلات

- الاحتفاظ بسجلات أنشطة المعالجة من قبل المتحكمين/المعالِجين.
- تطبيق تدابير حماية كافية لعمليات النقل عبر الحدود.
- اشتراط الالتزامات التعاقدية من المعالِجين تجاه معايير حماية البيانات قبل مشاركة البيانات الشخصية.

التزامات حماية البيانات

- تنفيذ التدابير التقنية والتنظيمية المناسبة، مع مراعاة المخاطر المرتبطة بمعالجة البيانات.
- الإبلاغ عن خروقات البيانات الشخصية خلال 72 ساعة إلى وزارة النقل والاتصالات وتقنية المعلومات والأفراد المتأثرين.
- تقييم أثر الخصوصية على أصحاب البيانات قبل القيام بعمليات النقل عبر الحدود.

الالتزامات المتعلقة بالامتثال

- تعيين مسؤول حماية البيانات الشخصية للإشراف على الامتثال لقانون حماية البيانات الشخصية.
- ضمان قيام كلٍّ من المتحكمين والمعالِجين بتعيين مدقق خارجي.
- الحصول على موافقة صريحة من أصحاب البيانات قبل نقل البيانات الشخصية خارج سلطنة عمان.

ما الذي يجب أن تقوم به الشركات؟

يمثل قانون حماية البيانات الشخصية تحولًا جوهريًا في كيفية تعامل المؤسسات مع جمع البيانات الشخصية ومعالجتها وإدارتها.
يمتد تأثيره ليشمل جميع القطاعات التي تتعامل مع المعلومات الشخصية، مما يتطلب من الشركات الانتقال من الامتثال التفاعلي إلى الحوكمة الاستباقية للبيانات الشخصية.
يوضح القسم التالي الاعتبارات الرئيسية والخطوات العملية لمساعدة المؤسسات على التنقل بفعالية في رحلة الامتثال لقانون حماية البيانات الشخصية، ومواءمة سياساتها وإجراءاتها وضوابطها مع متطلبات حماية البيانات، مع بناء الثقة في اقتصاد قائم على البيانات.

إمكانية الاطلاع على البيانات الشخصية

مع تزايد الاعتماد على التقنيات الرقمية في سلطنة عمان، تقوم المؤسسات بمعالجة بيانات شخصية أكثر من أي وقت مضى. يفرض قانون حماية البيانات الشخصية ولائحته التنفيذية واجبات صارمة على المتحكمين والمعالِجين، بدءًا من احترام حقوق الأفراد وصولًا إلى حماية البيانات الحساسة مثل المعلومات الصحية وبيانات الأطفال.
لضمان الامتثال، تحتاج الشركات إلى وضوح كامل بشأن كيفية انتقال البيانات الشخصية عبر أنظمتها. يبدأ ذلك بعملية شاملة لاكتشاف البيانات ورسم خرائطها لتحديد أماكن جمعها وتخزينها ومعالجتها ومشاركتها. هذا الوضوح يعد أساسًا لبناء برنامج خصوصية يفي بالمعايير القانونية ويعزز الثقة العامة.

إدارة الموافقات

يعترف قانون حماية البيانات الشخصية بالموافقة كأساس قانوني رئيسي لمعالجة البيانات الشخصية، مما يوجب على المؤسسات الحصول على موافقة صريحة من أصحاب البيانات قبل بدء أو مواصلة أنشطة المعالجة. وبالمثل، يجب أن يتمكن أصحاب البيانات من سحب موافقتهم من خلال آليات تكون بسيطة وسهلة الوصول مثل عملية تقديمها.
تشترط اللائحة التنفيذية الحصول على موافقة صريحة للأنشطة مثل التسويق والإعلانات. أما بالنسبة لبيانات الأطفال، فيجب أن تأتي الموافقة من ولي الأمر القانوني، ويجب أن تخدم جميع عمليات المعالجة مصلحة الطفل الفضلى بشكل واضح.
للامتثال، ينبغي على الشركات مراجعة وتعزيز ممارسات جمع وإدارة الموافقات، بما في ذلك ضمان أن تكون الموافقة مستنيرة ومحددة وواضحة، والحفاظ على سجلات قوية للموافقات، وتوفير آليات سحب واضحة وسهلة الاستخدام ويمكن الوصول إليها.

الحفاظ على حقوق الخصوصية للأفراد

بموجب قانون حماية البيانات الشخصية، يتم منح الأفراد حقوقًا شاملة فيما يتعلق ببياناتهم الشخصية، مما يمكّنهم من لعب دور نشط في كيفية جمع معلوماتهم واستخدامها والاحتفاظ بها. تشمل هذه الحقوق: الحق في الإعلام، الحق في الوصول، الحق في التصحيح أو التعديل، الحق في المسح، والحق في الاعتراض على المعالجة.
ويعني ذلك أن أصحاب البيانات يمكنهم طلب من المؤسسات تزويدهم بنسخة من بياناتهم الشخصية، وتصحيح أي أخطاء، أو حذف معلومات محددة. وتشترط اللوائح التنفيذية أن تستجيب المؤسسات لهذه الطلبات خلال 45 يومًا. وفي بعض الحالات، يجوز للمؤسسة رفض تلبية طلب صاحب البيانات (مثلًا إذا كان الطلب متكررًا بشكل غير مبرر أو يتطلب تنفيذه جهدًا استثنائيًا).

التعامل مع مخاوف نقل البيانات عبر الحدود

تخضع عمليات نقل البيانات الشخصية عبر الحدود لتنظيم صارم بموجب قانون حماية البيانات الشخصية في عُمان. يمكن للمؤسسات نقل البيانات إلى الخارج فقط إذا منح الفرد موافقة صريحة، وكانت الدولة أو الجهة المستقبِلة توفر معايير حماية بيانات تتوافق أو تتجاوز تلك التي يحددها القانون العُماني. كما يُلزَمون بتقييم المخاطر المرتبطة بهذه التحويلات قبل تنفيذها.
وبما أنه لم يتم إصدار قائمة رسمية بالدول المعتمدة، فإن أي تحويلات إلى جهات قضائية لا تتوفر فيها معايير حماية بيانات مكافئة تستوجب اتخاذ ضمانات إضافية لضمان الامتثال.
ينبغي على الشركات العاملة على مستوى عالمي أن تراجع بعناية ممارسات نقل البيانات الخاصة بها، وتُجري تقييمات للمخاطر، وتطبّق إجراءات تقنية وتنظيمية مناسبة، وتحتفظ بوثائق تُثبت أن جميع عمليات نقل البيانات عبر الحدود تمت وفقًا لقانون حماية البيانات الشخصية.

استخدام الأطراف الثالثة

بموجب قانون حماية البيانات الشخصية، يظل المتحكمون مسؤولين بالكامل عن البيانات الشخصية التي تتم مشاركتها مع معالِجين من الأطراف الثالثة. لذلك يجب على المؤسسات اعتماد نهج صارم لإدارة المورّدين لضمان الامتثال. قبل التعامل مع أي جهة خارجية، يجب على الشركات القيام بما يلي:
تقييم ممارسات حماية البيانات لدى المورّد ومستوى الأمان من خلال إجراءات العناية الواجبة المفصّلة.
إبرام اتفاقيات ملزمة توضح بوضوح نطاق المعالجة، شروط السرية، توقعات الأمان، وبروتوكولات الإبلاغ عن أي خرق.
الحصول على موافقة مسبقة لأي ترتيبات للتعاقد من الباطن لضمان الشفافية والإشراف.
تقييم أداء المورّد والامتثال بشكل دوري من خلال المراجعات أو التدقيقات المنتظمة.
الحفاظ على خطوط واضحة للمساءلة مع وزارة النقل والاتصالات وتقنية المعلومات، مع إدراك أن المعالِجين يجب أن يبلغوا عن أي خروقات، لكن المتحكم يتحمل المسؤولية النهائية لضمان المعالجة القانونية والآمنة للبيانات.

التزامات المتحكم في البيانات

بموجب قانون حماية البيانات الشخصية يتحمل المتحكمون في البيانات أي المؤسسات التي تحدد أهداف ووسائل معالجة البيانات الشخصية المسؤولية الأساسية لضمان الامتثال للقانون ولوائحه التنفيذية. يجب على المتحكمين اعتماد نهج استباقي قائم على تقييم المخاطر لحماية البيانات، مع ترسيخ مبدأ المساءلة في جميع العمليات.

تشمل الالتزامات الرئيسية ما يلي:

- التعاون مع الوزارة: يجب على المتحكم التعاون مع الوزارة من خلال تقديم البيانات والمستندات المطلوبة عند الطلب.
- تعيين مدقق خارجي: عند طلب الوزارة، يجب على المتحكم تعيين مدقق خارجي لتقييم الامتثال، وتقديم نتائج التدقيق رسميًا إلى الوزارة.
- المشروعية والإنصاف والشفافية: يجب أن تستند جميع أنشطة البيانات إلى أساس قانوني صحيح مثل الموافقة الصريحة، وأن يتم توضيحها للأفراد بشكل واضح.
- أمن البيانات: تنفيذ ضوابط تقنية وتنظيمية قوية لمنع الوصول غير المصرح به أو إساءة الاستخدام أو فقدان البيانات الشخصية.
- سجلات أنشطة المعالجة : الاحتفاظ بتوثيق مفصل لعمليات المعالجة، بما في ذلك أنواع البيانات، الأغراض، فترات الاحتفاظ، المستلمين، وأي عمليات نقل دولية.
- الحوكمة والإشراف: تعيين مسؤول حماية البيانات الشخصية والتعاون مع مدقق خارجي معتمد للإشراف على الامتثال وتقديم ضمانات مستقلة.
- إدارة المعالِجين: ضمان أن أي معالِجين خارجيين يعملون وفق شروط تعاقدية صارمة، ويتبعون التعليمات الموثقة، ويلتزمون بجميع متطلبات قانون
- إدارة حقوق أصحاب البيانات: التعامل بفعالية مع حقوق أصحاب البيانات من خلال ضمان الاستجابة في الوقت المناسب لطلبات الوصول، التصحيح، المسح، الاعتراض، وسحب الموافقة.
- الإبلاغ عن الخروقات: الإبلاغ عن أي خرق للبيانات الشخصية إلى الجهة التنظيمية خلال 72 ساعة، وفي حال كان الخرق قد يسبب ضررًا جسيمًا أو مخاطر عالية للأفراد المتأثرين، يجب إبلاغهم أيضًا خلال نفس الفترة مع تقديم تفاصيل الحادث والإجراءات المتخذة لاحتوائه أو الحد من تأثيره.

التزامات معالِج البيانات

بموجب قانون حماية البيانات الشخصية، يجب على المعالِجين الذين يتعاملون مع البيانات الشخصية نيابةً عن المتحكمين العمل ضمن حدود قانونية وتعاقدية صارمة. وعلى الرغم من أن المتحكمين يتحملون المسؤولية العامة، فإن المعالِجين مسؤولون بشكل مستقل عن الحفاظ على معايير حماية البيانات ودعم جهود الامتثال.

تشمل الالتزامات الرئيسية ما يلي:

- التعاون مع الوزارة: يجب على المعالِجين التعاون مع وزارة النقل والاتصالات وتقنية المعلومات من خلال تقديم السجلات والمستندات ذات الصلة عند الطلب.
- تعيين مدقق خارجي: عند طلب الوزارة، يجب على المعالِج تعيين مدقق خارجي للتحقق من الامتثال لإجراءات وضوابط المعالجة، وتقديم نسخة من تقرير المدقق إلى الوزارة.
- المعالجة القانونية وفق التعليمات: يجب معالجة البيانات الشخصية وفقًا للتعليمات الموثقة من المتحكم، والامتناع عن أي معالجة لأغراض غير مصرح بها.
- سجلات المعالجة: يجب الاحتفاظ بسجلات مفصلة لجميع عمليات المعالجة التي تتم لصالح المتحكمين، بما في ذلك أنواع البيانات، الغرض من المعالجة، المستلمين، وأي عمليات نقل عبر الحدود.

إخطار بخرق البيانات

بموجب قانون حماية البيانات الشخصية، يجب على المؤسسات الإبلاغ عن أي خرق للبيانات الشخصية إلى وزارة النقل والاتصالات وتقنية المعلومات خلال 72 ساعة من اكتشافه، إذا كان الحادث يشكل خطرًا على خصوصية أو سرية أو أمن الأفراد. وإذا كان الخرق من المحتمل أن يؤدي إلى ضرر جسيم أو خطر كبير على الأفراد، يجب أيضًا إخطار أصحاب البيانات المتأثرين دون تأخير، وعادةً خلال نفس الفترة البالغة 72 ساعة.

توفر اللائحة التنفيذية إرشادات حول معايير الإبلاغ عن الخروقات وآلية التواصل مع أصحاب البيانات.

وفي ضوء هذه المتطلبات، ينبغي على المؤسسات مراجعة وتعزيز برامج مراقبة الأمان وإدارة الحوادث لضمان الكشف المبكر عن الخروقات المحتملة. يجب دمج عمليات إدارة الحوادث مع الرقابة على الخصوصية، وتحديد الإجراءات بوضوح لضمان الإبلاغ عن الخروقات في الوقت المناسب وبما يتوافق مع قانون حماية البيانات الشخصية.

تعيين مسؤول حماية البيانات الشخصية

موجب قانون حماية البيانات الشخصية، يتعين على المتحكمين في البيانات تعيين مسؤول حماية البيانات الشخصية يكون مسؤولًا عن إدارة والإشراف على تنفيذ برنامج حماية البيانات الشخصية في المؤسسة وضمان الامتثال للقانون ولوائحه التنفيذية.

كما يُطلب من كل من المتحكمين والمعالِجين من قبل الوزارة تعيين مدقق خارجي لمراجعة الامتثال، وتقييم الضمانات، وتقديم تقارير دورية إلى الوزارة.

بالإضافة إلى هذه الأدوار الرسمية، ينبغي على المؤسسات إنشاء برنامج منظم لحماية الخصوصية لإدارة البيانات الشخصية بشكل مسؤول ومتسق. وتشمل العناصر الأساسية لهذا البرنامج ما يلي:

- إعداد أطر الحوكمة لتحديد وإدارة مخاطر الخصوصية.
- إنشاء وتحديث السياسات والإجراءات الداخلية بما يعكس الالتزامات القانونية.
- تحديد أدوار واضحة وخطوط للمساءلة بشأن حماية البيانات عبر الفرق المختلفة.
- دمج الخصوصية وإدارة المخاطر في الممارسات اليومية للتعامل مع البيانات.

من خلال ترسيخ هذه الممارسات، يمكن للشركات إنشاء نموذج امتثال قوي يلبي توقعات الجهات التنظيمية ويعزز الثقة طويلة الأمد مع العملاء والشركاء والجهات الرقابية.

كيف يمكننا في بروتيفيتي مساعدتكم؟

تساعد شركة بروتيفيتي المؤسسات في إدارة رحلتها نحو الامتثال لقانون حماية البيانات الشخصية من خلال نهج مرحلي منظم ومرن في الوقت نفسه. تم تصميم هذه المنهجية لمعالجة احتياجات العملاء الخاصة مع ضمان التوافق مع الالتزامات التنظيمية. يقوم نهجنا على أربع مراحل رئيسية توجه المؤسسات من التقييم الأولي مروراً بالتنفيذ وصولًا إلى المراقبة المستمرة.

من خلال تطبيق هذا الإطار، نجحت بروتيفيتي في دعم العديد من العملاء في إنشاء وتعزيز برامج الخصوصية لديهم، مما مكّنهم ليس فقط من تلبية متطلبات الامتثال، بل أيضًا من بناء ثقة مستدامة مع أصحاب المصلحة.

مدة كل مرحلة ومستوى الجهد المبذول يعتمدان بشكل كبير على طبيعة البيانات الشخصية التي تتم معالجتها، وحجم ونطاق بيئة المؤسسة، وتعقيد العمليات ومستوى نضجها.

نبذة عن شركة بروتيفيتي

بروفِتيتي (www.protiviti.com) هي شركة استشارات عالمية تقدم خبرات عميقة ورؤى موضوعية ونهجًا مخصصًا وتعاونًا لا مثيل له لمساعدة القادة على مواجهة المستقبل بثقة. توفر بروفِتيتي وشركاتها الأعضاء المستقلة والمحلية للعملاء خدمات الاستشارات والحلول المُدارة في مجالات التمويل والتكنولوجيا والعمليات والبيانات والرقمنة والقانون والموارد البشرية والمخاطر والتدقيق الداخلي، وذلك من خلال شبكة تضم أكثر من 90 مكتبًا في أكثر من 25 دولة.

تم إدراج بروفِتيتي في قائمة "أفضل 100 شركة للعمل بها" الصادرة عن مجلة فورتشن للسنة الحادية عشرة على التوالي. وقد قدمت الشركة خدماتها لأكثر من 80٪ من شركات فورتشن 100 وما يقارب 80٪ من شركات فورتشن 500. كما تعمل الشركة مع الجهات الحكومية والشركات الصغيرة والمتنامية، بما في ذلك تلك التي تسعى لطرح أسهمها للاكتتاب العام. بروفِتيتي إنك هي شركة تابعة بالكامل لشركة روبرت هاف (رمزها في بورصة نيويورك: RHI).

معلومات الاتصال

د.عبدالله البلوشي
المدير التنفيذي
+968 9203 0305
Abdullah.Albalushi@protivitiglobal.me

شذا المسكري
المدير التنفيذي
+968 99848584
Shatha.Maskiry@protivitiglobal.me

نيراج ماثور
المدير التنفيذي
+971 502547507
Niraj.Mathur@protivitiglobal.me

مكاتبنا في منطقة الشرق الأوسط وشمال أفريقيا

سلطنة عُمان
مبنى الأفق، الطابق الثاني، المكتب رقم 26
شاطئ القرم
ص.ب 1130، الرمز البريدي 112
روي، مسقط، سلطنة عُمان

أبوظبي
مبنى مؤسسة الإمارات العقارية،
الطابق السابع، المكاتب 707-711
شارع الفلاح، منطقة الدانة
ص.ب 32468 أبوظبي، الإمارات
العربية المتحدة

دبي
المكتب رقم 2104، الطابق الحادي
والعشرون
برج أبورا 2 الخليج التجاري
ص.ب 78475، دبي، الإمارات العربية
المتحدة

مصر
مجمع القاهرة
شارع أنقرة، المكتب 1، الطابق الأول
منطقة الشيراتون، هليوبوليس –
القاهرة، مصر

الكويت
برج الشهيد، الطابق الرابع
شارع خالد بن الوليد، شرق
ص.ب 1773، الصفاة 13018، الكويت

البحرين
برج بلاتينيوم، الطابق السابع عشر
ص.ب 10231، المنطقة الدبلوماسية
المنامة، مملكة البحرين

قطر
، الطابق التاسع عشرB برج النخلة
ص.ب 13374، الخليج الغربي
الدوحة، قطر

المملكة العربية السعودية –
الدمام
الحي التجاري، سلمان الفارسي، الربع
Q1-5 التجاري
الخالدية الجنوبية، الدمام، المنطقة
الشرقية، 32221
المملكة العربية السعودية

المملكة العربية السعودية – جدة
طريق الملك عبدالعزيز الفرعي
حي الشاطئ، مبنى رقم 7524
ص.ب 3675، جدة 23412
المملكة العربية السعودية

المملكة العربية
السعودية – الرياض
برج الإبداع، الطابق
التاسع والثامن عشر
طريق الملك فهد
الفرعي، العليا، مبنى
رقم 7906
ص.ب 3825، الرياض
12313
المملكة العربية
السعودية

تطلّع إلى المستقبل بثقة